UNITED SIGNALS

Technical & Organisational Measures to Art. 3 DSV (Art. 32 GDPR)

Organizations that collect, process, or use personal data themselves or on behalf of others must take the necessary technical and organizational measures to ensure compliance with data protection laws. Measures are only required if their effort is proportionate to the intended protection goal.

1. Confidentiality

1.1 Access Control

→ No unauthorized access to data processing facilities (building and room security):

☐ Magnetic or chip cards
☒ Keys
☒ Electric door openers
☒ Factory security or gatekeepers
☒ Alarm systems
☒ Video surveillance
☐ Automated access control system
☐ Locking system with code lock
☐ Manual locking system
☒ Security locks
☒ Key management (key issuance, etc.)
☐ Biometric access barriers
☐ Visitor logging
☒ Careful selection of cleaning staff
☒ Careful selection of security staff
☐ Mandatory wearing of ID badges
☒ Visitors are supervised
☒ Everyone knows everyone (SME)
☒ Access authorization structure is restricted to the necessary minimum

1.2 System Access Control

→ No unauthorized system use:

☒ (Secure) passwords
☒ Automatic monitor screen lock on
☒ Creation and enforcement of a password policy
☒ Two-factor authentication
☒ Encryption of storage media
☒ Assignment of user rights
☒ Creation of user profiles

☒ Authentication via username/password
☐ Case locks
☐ Use of VPN technology
☒ Disabling external interfaces (USB, etc.)
☐ Encryption of mobile storage devices
☐ Encryption of smartphone contents
☐ Use of centralized smartphone administration software
☒ Use of antivirus software
☒ Encryption of storage media in laptops/notebooks
☐ Use of hardware/software firewall
☒ Access authorization structure is restricted to the necessary minimum

1.3 Data Access Control

→ No unauthorized reading, copying, modification, or deletion within the system:

☒ Creation and enforcement of authorization concepts with tailored access rights
☒ Logging of access to applications: input, modification, and deletion
☒ Management of rights by a system administrator
☒ Reduction of the number of administrators
☒ Password policy including password length, change intervals
☒ Secure storage of storage media
☒ Secure wiping of storage media before reuse
☒ Proper destruction of storage media

1.4 Separation Control

→ Separate processing of data collected for different purposes:

☒ Physical storage separation on distinct systems or media
☒ Separation of production and test environments
☒ Software-based tenant separation
☒ Creation of an authorization concept
☒ Encryption of datasets processed for the same purpose
☒ For pseudonymized data: separation of the assignment file
☒ Definition of database rights

1.5 Pseudonymization

☐ Processing of personal data in a way that the data cannot be attributed to a specific data subject without additional information, provided this additional information is stored separately and subject to appropriate technical and organizational measures.

2. Integrity

2.1 Transfer Control

→ No unauthorized reading, copying, modification, or removal during electronic transmission or transport:

- ☐ Email encryption
- ☐ Virtual Private Networks (VPN)
- ☐ Electronic signature
- ☒ Logging of access and retrievals
- ☒ Provision via encrypted connections such as SFTP, HTTPS
- ☒ Transfer of personal data in anonymized or pseudonymized form
- ☐ Creation of an overview of regular retrieval and transmission processes
- ☒ Documentation of recipients of data and timeframes for planned handovers or agreed deletion deadlines
- ☐ For physical transport: secure transport containers/packaging

2.2 Input Control

→ Verification of whether, by whom, and when personal data has been entered, modified, or removed from data processing systems:

- ☒ Logging of the entry, modification, and deletion of personal data
- ☒ Document management
- ☒ Creation of an overview of which applications allow entry, modification, and deletion of personal data
- ☒ Traceability of entry, modification, and deletion of personal data through individual usernames
- ☐ Retention of forms from which personal data has been transferred to automated processing systems
- ☒ Assignment of rights to enter, modify, and delete personal data based on an authorization concept

3. Availability and Resilience

3.1 Availability Control

→ Protection against accidental or deliberate destruction or loss:

(Note: United Signals does not operate its own servers, so there is no server infrastructure to protect. We use SaaS solutions managed by third-party providers. The following measures refer to the solutions provided by our third-party vendors.)

- ☒ Backup strategy (online/offline; on-site/off-site)
- ☒ Uninterruptible power supply (UPS)
- ☒ Antivirus protection
- ☒ Firewall
- ☒ Reporting channels and emergency plans

- ☒ Rapid recoverability
- ☒ Air conditioning in server rooms
- ☒ Surge-protected power strips in server rooms
- ☒ Fire and smoke detection systems
- ☒ RAID-Systems / disk mirroring
- ☒ Alarm notifications for unauthorized access to server rooms
- ☒ Video surveillance in server rooms
- ☒ Monitoring of temperature and humidity in server rooms
- ☒ Creation of a backup concept
- ☒ Regular data recovery tests and logging of results
- ☒ Storage of backups in a secure, off-site location

4. Procedures for Regular Review, Assessment, and Evaluation

4.1 Data Protection Management

- ☒ Use of software solutions for data protection management
- ☒ Centralized documentation of all procedures and regulations concerning data protection, accessible to employees based on their needs/permissions (e.g., wiki, intranet)
- ☒ Security certification, such as SOC2
- ☒ Other documented security concepts
- ☒ Annual review of the effectiveness of technical security measures
- ☒ External data protection officer
- ☒ Employees trained and committed to confidentiality/data secrecy
- ☒ Regular employee awareness training, at least annually
- ☒ Internal/external information security officer
- ☒ Data protection impact assessment (DPIA) conducted as needed
- ☒ Compliance with information obligations under Articles 13 and 14 GDPR
- ☒ Formalized process for handling data subject access requests

4.2 Incident-Response-Management

- ☒ Use of firewalls with regular updates
- ☒ Use of spam filters with regular updates
- ☒ Use of antivirus scanners with regular updates
- ☒ Intrusion Detection System (IDS)
- ☒ Intrusion Prevention System (IPS)
- ☒ Regular software updates (patch and vulnerability management)
- ☒ Documented process for identifying and reporting security incidents/data breaches (including notification obligations to supervisory authorities)
- ☒ Documented procedures for handling security incidents
- ☒ Involvement of DPO and ISO in security incidents and data breaches
- ☒ Documentation of security incidents and data breaches (e.g., via ticketing system)
- ☒ Formal process and responsibilities for follow-up on security incidents and data breaches

4.3 Data Protection by Default

☒ Only personal data necessary for the respective purpose is collected
☒ Simple exercise of the data subject's right to withdraw consent through technical measures

4.4 Outsourcing Control (Third-Party Processing)

☒ Prior assessment of security measures taken by the processor and their documentation
☒ Selection of the processor based on due diligence (particularly concerning data protection and security)
☒ Conclusion of necessary data processing agreements or EU standard contractual clauses
☒ Written instructions to the processor
☒ Clear contractual arrangements
☒ Commitment of the processor's employees to data secrecy
☒ Obligation for the processor to appoint a data protection officer where legally required
☒ Agreement on effective audit rights for the processor
☒ Regulations for the use of subcontractors
☒ Assurance of data destruction after contract termination
☒ For long-term collaboration: ongoing review of the processor and its security level